

Patent Application Serial No. 10/767,842

REMARKS

Claims 3-5, 12, and 15 are now canceled without prejudice to reentry. Claims 1, 2, 11, and 13 are amended.

Claims 1-5, 11-13, and 15 remain rejected under 35 U.S.C. §103(a) as being obvious over US 6,950,943 to Bacha, previously applied. This rejection is respectfully traversed.

(1) In the Response to Arguments on page 2, the Examiner states that Bacha discloses two check codes made by an encryption algorithm unique to the system, and that the application running in the application server's vault then signs the document it has received (col. 6, line 64-65), as a first check code; and further states that the application running in the application servers' vault notarizes the signature (block 310) by re-signing it with its own private signing key (col. 6, lines 42-44), as a second check code.

The Examiner further asserts (§ 6 on page 3 of the Action) that Bacha discloses that a second code is created by an encrypting method unique to the system from the electronic signature for registration, because Bacha discloses that the application server's vault notarizes the signature block (block 310) by re-signing with its own private signing key (col. 6, lines 42-44).

Bacha discloses that **the encrypted document, the document originator's notarized signature, and the non-repudiation receipt** are all stored in the application server's repository or database (block 314) at col. 7, lines 9-12.

It is also disclosed that the notarized electronic signature contains the originator's signature of the given data element and the notary's signature of the originator's signature, which is computed over the originator's signature and the current time stamp (col. 6, lines 59-64).

Furthermore, it is disclosed that this second signature is computed over the encrypted document and the originator's notarized signature (col. 7, lines 1-3).

(2) However, in retrieving the document of Figs. 4A and 48, the Bacha application server's vault application receives the access request (block 404) and retrieves the encrypted document and the originator's notarized signature from application database (block 406), as described in column 7, lines 48-51; the originator's vault application decrypts the document (block 416) and verifies the notarized signature (block 418), described in column 8, lines 15-18.

Patent Application Serial No. 10/767,842

Furthermore, it is disclosed that since the originator's original signature was computed over the unencrypted document contents, "*only those users with access to the document contents (i.e., with the originator's private key) are able to verify the signature*" (col. 8, lines 18-20).

Thus, Bacha discloses just the Applicants' prior art of Fig. 13 and page 2, line 12 *ff*—and Bacha has the same drawback: it is necessary to re-create the electronic signature of all stored data when changing the signature key (specification page 4, lines 2-8) and does not achieve the Applicant's objects (page 4, line 24 to page 5, line 27).

(3) Thus, Bacha fails to disclose that an electronic signature for registration is created by encrypting a hash value of electronic data with a secret key; a second check code created by an encrypting method unique to the system from the electronic signature for registration; a controller that verifies the validity of the stored electronic data and the electronic signature by creating a third check code from the electronic data, by the encrypting method unique to the system; and a fourth code from the electronic signature for registration, by the encrypting method unique to the system.

(It is noted that Bacha does not use the word "registration." The closest mention in Bacha is that of "the IBM Vault Registry product, the subject of U.S. patent application Ser. No. 980,022," which is US Patent 6,105,131.)

Bacha fails to disclose comparing the stored first check code with the third check code and the stored second check code with the fourth check code.

Furthermore, Bacha fails to disclose or suggest outputting the electronic data, a second electronic signature created by encrypting the electronic data with a secret key which is valid at output time, and the electronic signature for registration when the compared result is favorable, as claimed.

The Applicants create a second check code by an encrypting method unique to the system from the electronic signature for registration when registration and the second check code is checked for output the document, and create a second electronic signature by encrypting the electronic data with a secret key which is valid at output time.

Patent Application Serial No. 10/767,842

Therefore, it is not necessary to change the electronic signature for registration when changing a public key. Bacha fails to teach this advantage, and the Applicants' features.

(4) The Examiner asserts (§ 5 on page 2) that the Applicants' two check codes are anticipated by two signatures of Bacha, a signature proper and a notarization of that signature. Bacha explains (col. 6, line 45) that "The notarization of a signature, in an electronic context, means that a third party, which acts as a 'notary', certifies the content of a signature. ... In the case of the present invention, notarization of the user's digital signature prevents the user from modifying the original document ... A notarized electronic signature contains two pieces of information, the originator's signature of the given data element and the notary's signature of the originator's signature. The notary's signature should be computed over the originator's signature and the current time stamp." That is, Bacha's notarizing is an electronic signature of an electronic signature.

Amended claim 1 recites "wherein said data processing unit generates [1] said first check code by an encrypting method unique to said system from said electronic data, [2] an electronic signature for registration by encrypting a hash value of said electronic data with a secret key, and [3] said second check code by an encrypting method unique to said system from said electronic signature for registration." According to the definition of the reference itself, only the third item, namely the second check code, can possibly anticipate the notarization of Bacha.

The first and second items in this portion of claim 1 are recited as a check code and an electronic signature. The Examiner asserts (Action at the bottom of page 2) that Bacha's "signatures" anticipate the claimed check codes, and explains (page 3, line 2) that Bacha's signature "is computed by encrypting a digest of a document ... Hence, ... Bacha expressly discloses two check codes made by an encryption algorithm unique to the system from hash values." The Examiner is understood to equate a check code to an electronic signature.

However, even granting the Examiner's assertion of equivalence, the first and second items above number two, and therefore there must a total of two check codes/signatures disclosed by the reference, in addition to the notarizing signature.

Patent Application Serial No. 10/767,842

(The Applicants are uncertain of whether the asserted equivalence of "check code" and "electronic signature" has been established. A search on Google Patents discovered thirteen patents with both "check code" and "electronic signature," implying that these terms can be distinguished in the art.)

The Examiner has not responded to the earlier argument concerning "unique to the system."

Claims 6-10 are rejected under 35 U.S.C. §103(a) as being obvious over Bacha in view of US 5,748,738 to Bisbee, previously applied. This rejection is respectfully traversed on the grounds above.

In view of the aforementioned amendments and accompanying remarks, the claims as amended are in condition for allowance, which action, at an early date, is requested.

Respectfully submitted,

KRATZ, QUINTOS & HANSON, LLP



Nick S. Bromer
Attorney for Applicant
Reg. No. 33,478

NSB/lrj
Atty. Docket No. 040033
Suite 400
1420 K Street, N.W.
Washington, D.C. 20005
(202) 659-2930

23850

PATENT & TRADEMARK OFFICE

I hereby certify that this correspondence is being facsimile transmitted to the Patent and Trademark Office (Fax No. (571-273-8300) on February 5, 2009.

Nick Bromer (reg. no. 33,478)

Signature 